

**DETEKSI MALWARE ANDROID BERDASARKAN SYSTEM CALL  
MENGUNAKAN ALGORITMA SUPPORT VECTOR MACHINE**

**Laporan Tugas Akhir**

Diajukan Untuk Memenuhi

Persyaratan Guna Meraih Gelar Sarjana Strata I

Teknik Informatika Universitas Muhammadiyah Malang



**Sendi Herlambang**

**201310370311011**

**JURUSAN TEKNIK INFORMATIKA**

**FAKULTAS TEKNIK**

**UNIVERSITAS MUHAMMADIYAH MALANG**

**2017**

**LEMBAR PERSETUJUAN**

**DETEKSI *MALWARE* ANDROID BERDASARKAN *SYSTEM CALL*  
MENGUNAKAN ALGORITMA *SUPPORT VECTOR MACHINE***

**Sendi Herlambang**

**201310370311011**


Telah Direkomendasikan Untuk Diajukan Sebagai  
Judul Tugas Akhir Di  
Teknik Informatika Universitas Muhammadiyah Malang

Menyetujui,

Dosen I,

Dosen II,

  
**Setio Basuki, ST., MT**  
**NIP : 108.0907.0477**

  
**Denar Regata Akbi, S.Kom, M. Kom**  
**NIP : 108.1612.0591**

## LEMBAR PENGESAHAN

### DETEKSI *MALWARE* ANDROID BERDASARKAN *SYSTEM CALL* MENGUNAKAN *ALGORTIMA SUPPORT VECTOR MACHINE*

#### TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1  
Teknik Informatika Universitas Muhammadiyah Malang

Disusun Oleh:

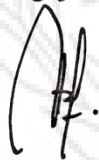
**Sendi Herlambang**

**201310370311011**

Tugas Akhir ini telah diuji dan dinyatakan lulus melalui sidang majelis penguji  
pada tanggal 25 Oktober 2017

Menyetujui,

Penguji I



**Mahar Faiqurahman, S.Kom., M.T.**

**NIP: 108.0811.0462**

Penguji II

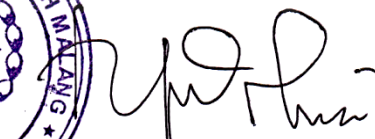


**Sofyan Arifianto, S.Si., M.Kom.**

**NIDN : 0721058309**

Mengetahui

Ketua Jurusan Teknik Informatika



**Yuda Munarko, S.Kom, M.Sc**

**NIP: 108.0611.0**

## LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

**NAMA : SENDI HERLAMBAANG**  
**NIM : 201310370311011**  
**FAK./JUR. : TEKNIK / INFORMATIKA**

Dengan ini saya menyatakan bahwa Tugas Akhir dengan Judul “**Deteksi Malware Android Berdasarkan System Call Menggunakan Algoritma Support Vector Machine**” beserta seluruh isinya adalah karya saya sendiri dan bukan merupakan karya tulis orang lain, baik sebagian maupun seluruhnya, kecuali dalam bentuk kutipan yang telah disebutkan sumbernya.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya. Apabila kemudian ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya ini, atau ada klaim dari pihak lain terhadap keaslian karya saya ini maka saya siap menanggung segala bentuk resiko/sangsi yang berlaku.

Malang, 10 Oktober 2017

Yang Membuat Pernyataan



**Sendi Herlambang**

**NIM : 201310370311011**

Dosen I,

**Setjo Basuki, ST., MT**  
**NIP : 108.0907.0477**

Dosen II,

**Denar Regata Akbi, S.Kom, M. Kom**  
**NIP : 108.1612.0591**

## KATA PENGANTAR

*Bismillaahirrahmaanirrahiim*

Segala puji dan syukur atas kehadiran Allah SWT yang telah memberikan karunia, rahmat dan hidayah-Nya sehingga penulis mampu menyelesaikan skripsi dengan judul “**Deteksi Malware Android Berdasarkan System Call Menggunakan Algoritma Support Vector Machine**” ini dengan baik. Skripsi ini berisi tentang melakukan teknik klasifikasi jenis *malware* Android dengan menggunakan algoritma *Support Vector Machine*.

Tujuan skripsi ini adalah dapat membagi beberapa jenis malware Android menjadi beberapa kelas dengan algoritma *Support Vector Machine*.

Penulis menyadari bahwa penulisan skripsi ini tidak terlepas dari dukungan, motivasi maupun bimbingan daari berbagai pihak. Akhirnya, penulis menyampaikan banyak terima kasih kepada, dosen pembimbing, dosen penguji dan teman-teman yang telah banyak membantu sehingaa skripsi ini bisa terselesaikan.

Penulis menyadari bahwa skripsi ini masih jauh dari kesempurnaan dan banyak mengandung kekurangan. Oleh karena itu penulis mengharapkan kritik dan saran yang membangun untuk tercapainya hasil penulisan yang lebih baik di masa yang akan datang. Akhir kata, semoga skripsi ini dapat memberikan manfaat bagi semua pihak yang membacanya.

Malang, 9 Oktober 2017

Penulis

## DAFTAR ISI

HALAMAN JUDUL.....	i
LEMBAR PERSETUJUAN.....	ii
LEMBAR PENGESAHAN .....	iii
LEMBAR PERNYATAAN KEASLIAN .....	iv
ABSTRAK .....	v
ABSTRACT.....	vi
KATA PENGANTAR .....	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR .....	xi
DAFTAR TABEL.....	xiii
BAB I PENDAHULUAN .....	1
1.1. Latar Belakang .....	1
1.2. Rumusan Masalah .....	3
1.3. Tujuan.....	3
1.4. Batasan Masalah.....	3
1.5. Metodologi .....	4
1.6. Sistematika Penulisan.....	6
BAB II LANDASAN TEORI .....	8
2.1. Sistem Operasi Android .....	8
2.1.1. Sejarah Android.....	9
2.1.2. Platform Android.....	9
2.1.3. Fitur Pada Android .....	10
2.1.4. Arsitektur Pada Android.....	11
2.2. System Call .....	12

2.3. Data Mining.....	14
2.3.1. Tugas Utama Data Mining .....	14
2.3.2. Proses Data Mining .....	15
2.4. Klasifikasi.....	16
2.4.1. Tujuan Klasifikasi .....	17
2.5. Malware.....	17
2.5.1. Jenis Jenis Malware.....	18
2.6. Support Vector Machine .....	18
2.6.1. Konsep Support Vector Machine .....	19
2.6.2. Multiclass Support Vector Machine.....	20
2.6.3. Kelebihan Support Vector Machine .....	20
2.6.4. Kekurangan Support Vector Machine .....	21
2.7. WEKA ( <i>Waikato Environment for Knowledge Analysis</i> ) .....	21
<b>BAB III ANALISA DAN PERANCANGAN SISTEM.....</b>	<b>23</b>
3.1. Data Penelitian .....	23
3.2. Mendapatkan System Call.....	23
3.3. Praproses Data.....	24
3.3.1. Seleksi Fitur.....	25
3.4. Pelatihan Data .....	25
3.5. Pengolahan Data Dalam Pengujian .....	28
3.6. Pengujian Klasifikasi.....	29
<b>BAB IV IMPLEMENTASI DAN PENGUJIAN.....</b>	<b>30</b>
4.1. Data Eksperimen .....	30
4.1.1. Persiapan Data.....	30
4.1.2. Preprocessing Data.....	31
4.2. Alur Implementasi.....	34
4.3. Seleksi Fitur.....	35
4.4. Hasil Cross Validation .....	36
4.5. Proses Support Vector Machine.....	38
4.6. Proses Klasifikasi .....	43

4.7. Hasil Analisa dari Proses Klasifikasi .....	44
BAB V PENUTUP.....	46
5.1. Kesimpulan.....	46
5.2. Saran.....	46
DAFTAR PUSTAKA .....	48





## DAFTAR GAMBAR

Gambar 1.1 Konsep SVM .....	5
Gambar 1.2 Arsitektur sistem untuk klasifikasi .....	5
Gambar 2.1 Arsitektur Android .....	11
Gambar 2.2 Proses aplikasi mengirimkan permintaan.....	13
Gambar 2.3 Tahap proses klasifikasi .....	17
Gambar 2.4 Proses cara kerja <i>Support Vector Machine</i> .....	19
Gambar 3.1 Proses pengambilan informasi <i>System Call</i> .....	23
Gambar 3.2 Tampilan program untuk mengubah file.....	24
Gambar 3.3 <i>Flowchart</i> seleskfi fitur .....	25
Gambar 3.4 Arsitektur system untuk klasifikasi.....	26
Gambar 3.5 <i>Flowchart</i> pengujian menggunakan <i>Support Vector Machine</i> .....	27
Gambar 3.6 Contoh iterasi data dengan <i>k-fold cross validation</i> .....	29
Gambar 4.1 Perintah untuk memulai program ADB .....	31
Gambar 4.2 Perintah untuk menampilkan proses yang sedang berjalan.....	31
Gambar 4.3 PID dari aplikasi yang akan diamati .....	32
Gambar 4.4 <i>System call</i> yang dipanggil dan disimpan ke dalam file .txt .....	32
Gambar 4.5 Tampilan program untuk mengubah file <i>system call</i> .....	33
Gambar 4.6 <i>Flowchart</i> program.....	33
Gambar 4.7 Alur Implementasi.....	35
Gambar 4.8 Hasil fitur yang terpilih menggunakan seleksi fitur .....	36
Gambar 4.9 Hasil <i>cross validation</i> data dengan seleksi fitur.....	37
Gambar 4.10 Hasil <i>cross validation</i> data tanpa seleksi fitur.....	37
Gambar 4.11 Grafik Hasil <i>Cross Validation</i> .....	38
Gambar 4.12 Klasifikasi kelas Adware dan Droidkungfu .....	39
Gambar 4.13Klasifikasi kelas Adware dan Plankton.....	39
Gambar 4.14 Klasifikasi kelas Adware dan Trojan .....	40
Gambar 4.15 Klasifikasi Droidkungfu dan Plankton.....	40
Gambar 4.16 Klasifikasi Droidkungku dan Trojan.....	41

Gambar 4.17 Klasifikasi Plankton dan Trojan .....	41
Gambar 4.18 Waktu yang dibutuhkan data tanpa seleksi fitur .....	42
Gambar 4.19 Waktu yang dibutuhkan data dengan seleksi fitur .....	42
Gambar 4.20 Hasil pelatihan data latih dengan algoritma SVM .....	42
Gambar 4.21 Grafik Hasil Klasifikasi Jenis <i>Malware</i> .....	44



## DAFTAR TABEL

Tabel 2.1 Data yang terkumpul selama periode 6 Maret 2017 .....	9
Tabel 3.1 File system call berupa matrik .....	28
Tabel 4.1 Pembagian Jumlah Data <i>Malware</i> .....	33
Tabel 4.2 Hasil keluaran dari program menjadi matriks.....	35
Tabel 4.3 Hasil akurasi data tanpa seleksi fitur .....	40
Tabel 4.4 Hasil akurasi data dengan seleksi fitur.....	40



## DAFTAR PUSTAKA

- [1] Yunus, Mohammad. 2009. Pendeteksian Malware Dengan Menggunakan Algoritma Multi-Naive Bayes. Tugas Akhir Jurusan Teknik Informatika Institut Teknologi Sepuluh November.
- [2] Kramer, S., & Bradfield, J. C. 2009. A general definition of malware. *Journal in Computer Virology*, 6(2), 105–114.
- [3] Kolbitsch, C., Comparetti, P. M., Kruegel, C., Kirda, E., Zhou, X., Wang, X., Antipolis, S. (n.d.). 2009. Effective and Efficient Malware Detection at the End Host. USENIX Association Berkeley. Montreal, Canada.
- [4] Baltaci Nuray, dkk. 2014. The Analysis of Feature Selection Methods and Classification Algorithms in Permission Based Android Malware Detection. Cyber Defense and Security Laboratory of METU-COMODO, Informatics Institute Middle East Technical University (METU), Ankara, Turkey.
- [5] Li Xiang, dkk. 2016. AN Android Malware Detection Method Based on Androidmanifest File. Beijing University of Posts and Telecommunications, Beijing 100876, China.
- [6] Fan Ming, dkk. 2016. Frequent Subgraph based Familial Classification of Android Malware. Department of Computer, The Hong Kong Polytechnic University, 999077, China.
- [7] Xiao Xi, dkk. Back-propagation neural network on Markov chains from system call sequences: a new approach for detecting Android malware with system call sequences. 1Graduate School at Shenzhen, Tsinghua University, 518055 Shenzhen, People's Republic of China.
- [8] Shifu Hou, dkk. 2016. Deep4MalDroid: A Deep Learning Framework for Android Malware Detection Based on Linux Kernel System Call Graphs. Department of Computer Science and Electrical Engineering West Virginia University Morgantown, WV, 26506, USA.
- [9] Vapnik, V dan Cortes, C. 1995. Support Vector Networks. *Machine Learning*, 20, 273-297.

- [10] Cristianini N, Taylor JS. (2000). An Introduction to Support Vector Machine and Other Kernel-based Learning Methods. Cambridge (GB): Cambridge University Press.
- [11] F. Tchakounté and P. Dayang, 2013. System Calls Analysis of Malwares on Android. vol. 2, no. 9, pp. 669–674.
- [12] Wahanggara Victor dan Yudi Prayudi. 2015. Malware Detection Through Call System on Android Smartphone Using Vector Machine Method. Jurnal Teknik Industri Universitas Islam Indonesia.
- [13] A. S. Nugroho, A. B. Witarto, and D. Handoko. 2008. Support Vector Machine. Jakarta.
- [14] DiMarzio, JF. 2008. Android A Programmer's Guide. USA: The McGraw-Hill Companies.
- [15] Nazaruddin Safaat H, 2013. Aplikasi Berbasis Android. Penerbit Informatika. Bandung.
- [16] Collins, C., Galpin, M.D. & Kappler, M. 2012. Android in Practice. Manning: Shelter Island, New York.
- [17] Anonymous, 2017. Android operating system data. (online) <https://developer.android.com/about/dashboards/index.html> Diakses pada 12 Maret 2017.
- [18] Gargenta, M. 2011. Learning Android. USA: O'Reilly Media.
- [19] Oktaviyan, Ragil. 2013. Rancang Bangun Aplikasi Android Untuk Menghitung Biaya Listrik Rumah Tangga. Fakultas Teknik. Universitas Negeri Semarang. Semarang.
- [20] Octafian, D. Tri. 2011. Desain Database Sistem Informasi Penjualan Barang. Jurnal Teknologi dan Informatika (TEKNOMATIKA). No. 2. Vol. 1.
- [21] Bergstra JA, Polse A. (2001). Register-machine based processes. Journal of the ACM.
- [22] M. Jones, 2007. Anatomy of the Linux kernel. (online) <https://www.ibm.com/developerworks/linux/library/l-linux-kernel/> , diakses pada 14 Mei 2017.
- [23] Nazaruddin Safaat H, 2013. Aplikasi Berbasis Android. Penerbit

Informatika. Bandung.

- [24] Burguera I. 2011. Behavior-based malware detection system for the android platform [tesis]. Linköping (SE): Linköping University.
- [25] Han, J and Kamber, M. 2006. Data Mining: Concepts and Techniques, Second Edition. Morgan Kauffman Publishers.
- [26] Santosa, B. 2007. Data Mining Teknik Pemanfaatan Data untuk Keperluan Bisnis. Yogyakarta. Graha Ilmu.
- [27] Sahu, H., Shirma, S. & Gondhalakar, S. 2011. A Brief Overview on Data Mining Survey. International Journal of Computer Technology and Electronics Engineering 1(3).
- [28] Kantardzic, M., 2003. Data Mining: Concepts, Models, Methods, And Algorithms. The Institute of Electrical and Electronics Engineers, Inc.
- [29] Carbonell, J.G., Michalski, R.S., & Mitchell, T.M. 1983. An Overview Of Machine Learning, In R.S. Palo Alto: Tioga Publishing Company.
- [30] Mining, P. D. (n.d.). Decision Tree Program Studi Informatika / Matematika, 1–6.
- [31] Hamkonda, Towa P dan Tairas. 1982. Pengantar Klasifikasi Persepuluhan Dewey. Jakarta : Gunung Mulia.
- [32] Basuki, Sulisty. 1911. Pengantar Ilmu Perpustakaan. Jakarta: Gramedia.
- [33] Milošević, N. 2013. History of Malware. Computer Security, pp 1.
- [34] Hastie Trevor, Robert Tibshirani, Jerome Friedman. 2008. The Elements of Statistical Learning Data Mining, Inference, and Prediction. Springer. Stanford, California.
- [35] Anto Satriyo Nugroho, Arief Budi Witarto, Dwi Handoko. 2003. Support Vector Machine Teori dan Aplikasinya dalam Bioinformatika. Kuliah Umum IlmuKomputer.com.
- [36] Witten, Ian H & Frank, Eibe., 2005. “Data Mining: Partical Machine Learning Tools and Technique 2<sup>nd</sup> Edition”. USA: Morgan Kaufman Publisher. Pp. 365-366.
- [37] Anonymous, 2017. Android operating system data. (online) <https://weka.wikispaces.com/Use+Weka+in+your+Java+code> Diakses pada 5 November 2017.

- [38] Gorunescu, F. (2011). Data Mining Concept Model Technique.
- [39] Chen, J., Huang, H., Tian, S., & Qu, Y. (2009). Feature selection for text classification with Naïve Bayes. *Expert Systems with Applications*, 36(3), 5432–5435.
- [40] Anggraeni Dyta. 2008. Klasifikasi Topik Menggunakan Metode Naive Bayes Dan Maximum Entropy Pada Artikel Media Massa Dan Abstrak Tulisan. Skripsi Sarjana pada Fakultas Ilmu Komputer Universitas Indonesia: tidak diterbitkan.
- [41] R. Kohavi, 1995. A study of Cross-Validation and Bootstrap for Accuracy Estimation and Model Selection. Computer Science Department Stanford University.

